

これまでの会合における 御指摘と対応案

令和8年2月9日

内閣官房
国家サイバー統括室
人材政策班



人材フレームワーク策定及び利活用等の基本的考え方(案) についての御意見

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 我が国における人材フレームワーク策定及び利活用等の基本的考え方(案)</p>	<p>民間企業の情報システム部門ではフレームワークとしてITSSを参照しているところが多いと思われるので、現場が混乱しないように配慮すべき。</p>	<p>既存のITSSのレベルとフレームワーク本体で定義するレベルの対応付けを明確化</p>	<p>役割の詳細のうち、レベル定義 各手引き書におけるレベル説明箇所</p>
	<p>フレームワーク策定の目的と、想定する利用者を明確にすべき。</p>	<p>手引き書において、フレームワーク策定の目的及び手引き書とフレームワーク本体の対応関係について整理</p>	<p>手引き書共通事項</p>
<p><第1回> 論点①：活用を見据えた人材像の設定</p>	<p>サイバーセキュリティ分野では技術的なところが注目されがちであるが、実際に活動する上では経営層ほか相手に応じて説明し、理解してもらう能力が重要。</p>	<p>マネジメント力やコミュニケーションスキルについてもフレームワーク本体で定義するレベルの設定において考慮</p>	<p>レベル定義</p>
	<p>利活用で活躍する人材の要件として、必要なスキルレベルを備えた上で、マネジメント力やプレゼンテーション力の発揮をプラスした表現ができるとうい。</p>		
	<p>技術的なスキルだけでなく、コミュニケーション・プレゼンテーションスキルについても言及・考慮があるとよい。</p>		

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 論点①：活用を見据えた人材像の設定(続き)</p>	<p>NICEは細かいが複数のロールの組合せで柔軟な表現ができる。特定の人材像を決めつけてしまうと日本では画一的にそれを目指して視野が狭い人材になりがち。</p>	<p>フレームワーク本体では、サイバーセキュリティ対策における汎用的な役割とし、手引き書において組織・業務特性に応じて、人材像をそれぞれ設定するという位置づけで整理</p>	<p>フレームワーク及び手引き書全体</p>
	<p>人材像およびレベルとそれに紐付く職種名が紐付くように、また、名は体を表すものとすべき。</p>	<p>資料2において、一部の役割の名称をより担当内容を具体的に表現可能な名称に見直しを実施。</p>	<p>役割の詳細のうち、各役割の名称</p>
	<p>育てる側と育てられる側、雇う側と雇われる側双方から見て共創的でなければならず、ほしい人材になりたい人材のギャップがあるのであれば、そういったところを調査する必要があるのではないか。</p>	<p>個人向け手引き書への反映に向けて、キャリアマップ等の整理を実施する。</p>	<p>個人向け手引き書全体</p>
	<p>幅広く企業に浸透させるには、企業の業務にプラスして、セキュリティとして何に取り組むべきかを定義するのがよい。</p>	<p>小規模組織向け及び個人向け手引き書においてプラス・セキュリティ人材として求められる知識・スキルの整理を実施予定</p>	<p>小規模組織向け及び個人向け手引き書</p>
<p><第1回> 論点②：既存の国内外のフレームワーク類との相互参照性の確保</p>	<p>妥当。大まかな役割を示すにとどめ、必要な知識などはSecBoKと紐付けるとわかりやすい。</p>	<p>SecBoKのほか、複数の人材フレームワークとの相互参照を可能とすることで、求められる知識に関する詳細を把握可能とする。</p>	<p>役割の詳細のうち、他のフレームワークとの相互参照</p>

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 論点②：既存の国内外のフレームワーク類との相互参照性の確保(続き)</p>	<p>ハブとすることで相互参照でき妥当であるが、NICEはかなり細かいので、参考にする場合は工夫が必要(類と小分類、カテゴリとサブカテゴリとなるような表現が整理し易くて良い)。</p> <p>様々なフレームワークの活動の活性化は望ましいが、その共通語として対応関係の目安が示せることが重要。ただし細かすぎると融通が利かなくなるのでよい落とし所を探るとよい。</p> <p>大手、中小企業それぞれについて、フレームワーク上の相互参照先となる企業間での役割分担を定義しておくべき。その整理ができていると何を定義すればよいか判断しやすくなる。</p>	<p>13の役割に対して、NICEのロールを基準として、NICEの各タスク(T)・知識(K)・スキル(S)を中項目レベルでサマライズした分類を実施</p> <p>SecBoKのほか、複数の人材フレームワークとの相互参照を可能とすることで、求められる知識に関する詳細を把握可能とする。</p> <p>外部委託を含めて外部組織との連携関係は手引き書にてモデルケースをもとに例示する</p>	<p>役割の詳細のうち、他のフレームワークとの相互参照</p> <p>役割の詳細のうち、他のフレームワークとの相互参照</p> <p>大規模組織向け手引き書におけるサプライチェーンでの利用に関する説明箇所</p>
<p><第1回> 論点③：フレームワークの性質</p>	<p>我が国のサイバーセキュリティ推進における共通理念を元とした議論が肝要。</p>	<p>我が国のサイバーセキュリティ推進における共通理念となるべく、サイバーセキュリティ対応における13の役割をフレームワーク本体にて整理</p>	<p>役割の詳細(将来的な拡張)</p>

御指摘と対応案(4/5)

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<第1回> 論点③：フレームワークの性質	実際の活用例、事例を手引き書に掲載してはどうか。	手引き書にてモデルケースを示し、フレームワークの活用例及び事例を提示	各種手引き書
	大企業や中小企業での役割の割り振りや、インソース、アウトソースの配分の参考となるものがあるとい	手引き書にてモデルケースを示し、フレームワークの活用例及び事例を提示	各種手引き書
	組織内部の人材の評価を行い、どこまでを自組織でまかない、どこから外部に委託するか見える化できるようなものもよい。		
<第1回> 論点④：策定後の利活用等	キャリアパス、キャリアプランを同時に示すことが大切である。	個人向け手引き書への反映に向けて、キャリアマップ等の整理を実施する。	個人向け手引き書全体
	策定後のプロモーションが大切である。	活用促進に向けて不断に検討を実施する	策定後の利活用
	教育をする際は、その人材や所属チームの役割（ミッション）に必要となる知識項目を意識する必要があり、定義する人材像ごとに必要となる主な知識項目をSecBoKとマッピングしておく使いやすい。	フレームワークにおいて定義された13の役割ごとに必要とされるスキル・知識を整理、教育機関向け手引き書において、これらを踏まえながら人材育成のカリキュラム設計に関する考え方を示す予定。 また、SecBoKとの対応については別途フレームワーク本体にて整理	役割の詳細のうち、他のフレームワークとの相互参照
	フォレンジック、捜査、脆弱性診断を提供する企業との間でフレームワークを軸とする相互参照ができるとよい。	各種フレームワークの共通言語となるべく、セキュリティ対応業務を13の役割として定義	

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 論点④：策定後の利活用等(続き)</p>	<p>サイバーセキュリティを他人事と捉えるマインドが脆弱性となっており、人材像に共通の横串を刺すようなものとして、自分事と捉えるマインドセットの醸成をフレームワークで定義できるとよい。</p> <p>企業内でサイバーセキュリティ対策を担う人材が、それぞれの部署(IT部門、総務部門、企画部門等)で自分がどの役割を担っているかが見える絵を描くことで、議論が進むのではないか。</p>	<p>手引き書にて組織規模別のモデルケースを示し、それらを通じた必要な役割について組織・人員の連携の事例を示す。</p>	<p>各手引き書におけるモデルケース</p>
<p><第1回> 論点⑤：「人材像」の呼称について</p>	<p>「人材像」なのか、「ロール」なのか、明確にしないと混乱させてしまう可能性がある。</p> <p>よく使われ、馴染みもある言葉でありかつ日本語であるので「人材像」が良いと思う。</p> <p>職務として行うべき機能だったり、実施すべき対処の大項目ととらえることが出来る名称が良く、機能とか役割のほうが日本では受け入れやすいのではないか。</p>	<p>フレームワーク本体において、サイバーセキュリティ対策に必要な役割として汎用的なものを整理し、それを踏まえて各組織特性を踏まえた人材像を設定する形に全体の構成を整理</p>	<p>「役割」についての説明箇所</p>

役割の設定(案)についての御意見

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 論点①：人材像定義やレベル設定の妥当性</p>	<p>①～⑯では人材の質が大きく異なる。たとえば、②～⑦は専任人材の色が強い。また、エンジニアリング系とマネジメント系が混在している。このような中、①～⑯を同じ色(グルーピング)としていることに違和感がある。</p>	<p>NICEのフレームワーク分類に基づきそれぞれの役割についてカテゴリ分けを実施。</p>	<p>役割定義のうち、役割一覧</p>
	<p>15の人材について、①従来からのセキュリティ専門家、②セキュリティ専門ではないがセキュリティに関する業務を行う人材、③他の業務を担いながら、セキュリティ視点のスキルも必要な人材、くらの3つにグルーピングするとわかりやすくなるのではないか。</p>	<p>個人向け手引書として、専門人材だけではなく、プラス・セキュリティ人材向け手引き書を作成することで、②や③の人材向けの考え方を整理予定</p>	<p>小規模組織向け手引き書における担当割り当ての説明箇所 プラス・セキュリティに取り組む個人向け手引き書における人材像の説明箇所</p>
	<p>数や粒度、レベルは示されている程度が限界かと思う。日本の場合、現実的には総合職的(メンバーシップ型)になるため、ジョブ例は5から10程度が理解を得られやすいのではないか。レベル設定は妥当。</p>	<p>実施する対象組織において13の役割でそれぞれ求められる内容を整理する形で対応し、各組織ごとに最低限役割を果たすために必要なスキルを組織向け手引き書にて整理予定。</p>	
	<p>汎用性があり、主要な人材像の設定は妥当。どんな定義や設定をしても不足は出るので、業種や組織に合わせたカスタマイズの仕方などを「手引き書」に示せるかどうかではないか。</p>	<p>御指摘の通り手引き書にて対応</p>	<p>小規模組織向け手引き書における企業の特徴の考慮に関する説明箇所</p>

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 論点①：人材像定義やレベル設定の妥当性(続き)</p>	<p>NICEのワークロールは、生成AIによる対応や自動化の適用可否を判断しやすい。15の人材像は役割説明がぼやけてどこに自動化の要素があるかが見づらくなっている。人が役割を担わない可能性を意識できるような説明になっているとよい。</p>	<p>AI関連のスキルについては、NICEの改定内容を踏まえて、一部フレームワーク側での取り込みを実施</p>	<p>役割の詳細のうち、主な業務及びタスクの定義</p>
<p><第1回> 論点①のうち、15の人材像の個別定義について</p>	<p>まだ存在しないものを作りだし、世の中の課題を解決するような人材像を示せないか。</p>	<p>13の役割の全体像を整理するうえで、研究の役割について全役割を下支えする形で、その位置づけを整理</p>	<p>役割の詳細のうち、要求される知識及びスキルの定義</p>
	<p>開発を担う人材像はアーキテクチャを担う人材層がすべて決めたものをコーディングするだけのように見えるが、現実には地政学上のリスクを捉えたアーキテクチャを分解した開発が行われるべきで、感覚がずれている印象を受ける。</p>	<p>ご意見を踏まえ、開発の名称を設計開発に変更</p>	<p>役割の詳細のうち、区分方法及び主な業務の定義</p>
	<p>最新のNICEでは国防関連の2つのカテゴリ(サイバースペースインテリジェンス、サイバースペースエフェクト)が除外されたが、OSINT能力に関するものが含まれてよいかを再検討すべき。</p>	<p>調査・情報収集の役割の中に内包する形で整理</p>	<p>役割の詳細のうち、タスク、要求される知識及びスキルの定義</p>

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第1回> 論点②：兼務実態への対応</p>	<p>現実的な兼務例をガイドラインで提示するのは効果的である。</p>	<p>組織向け手引き書において、モデルケースを示し、組織特性を踏まえてそれぞれの役割ごとの対応方法に関する一例を示す。</p>	<p>大規模・小規模組織向け手引き書</p>
	<p>職責分離の原則に反する兼務はダメであることの明示と例示が重要ではないか。</p>		
<p><第1回> 論点③：セキュリティ専門人材だけでなくプラス・セキュリティ人材の育成・確保</p>	<p>プラス・セキュリティまでこのフレームワークで取り扱うことは無理があり、経産省が進めているデジタルスキル標準と連携していくのがよいのではないか。</p>	<p>各組織向け手引き書において、モデルケースを示し、プラス・セキュリティ人材相当の人員も含めて役割を分担しながら果たす体制の一例を記載。また、個人向け手引き書として、専門人材だけでなく、プラス・セキュリティ人材向け手引き書を作成する。</p>	<p>プラス・セキュリティに取り組む個人向け手引き書</p>
	<p>プラス・セキュリティについて、あえて明確な定義はしていないが、先ほどの準コア、非コアについては、プラス・セキュリティ人材といえるかもしれない。また、デジタルスキル標準(DX推進人材)で定義されている部分も、ユーザ部分に存在するプラス・セキュリティ人材である。</p>		
	<p>コアを担う高度な人材像と、プラス・セキュリティの人材像とでは役割の重さが変わってくることもあり、それが読者に伝わるようにできるとよい。</p>		

御指摘と対応(4/4)

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第2回> 人材像(案)の 修正案について</p>	<p>長期的観点から、中核的なセキュリティ技術に関わる人材が我が国のどこで作れるかがフレームワークでわかるといいますが、資料からは研究開発等、高度な人材が活躍しそうなどが見えてこない。学生がこのフレームワークを見て、セキュリティ人材として生きていきたいと思えるようなものにしたい。</p>	<p>研究の役割が担うべき主要業務をフレームワークにおいて拡充し、特に専門人材向け手引き書において、トップ研究者等のキャリアマップを例示として示す。</p>	<p>専門人材を目指す個人向け手引き書</p>
	<p>①の人材像の説明にある「何々相当」というのは非常に分かりやすいが、他の人材像には書かれていない。またNICEフレームワークの対応ロールはあるが、実際にそれが何と呼ばれている仕事かが示されていない。これらがあるとイメージもしやすくなり、職種とも紐づくのでよいと思う。</p>	<p>御指摘の内容についてフレームワーク本体にて対応済み</p>	<p>役割の詳細のうち、役割及び想定される役職名等</p>
	<p>このような文書で相互理解を深め、「こういう人材が欲しい」と自社に必要な人材を明確にし、この人材が自社にいるかどうかの認識を共通言語として持てるものを目指してほしい。理想論かもしれないが、どこまでを最低限用意すべきか、どこからを外部委託するかをある程度示せるとよい。</p>	<p>13の役割に対して各組織別の手引き書で、求められる役割を具体的に定義・明確化し、小規模組織向け手引き書では、モデルケースをもとに最低限必要となるスキル・知識について整理</p>	<p>大規模組織向け手引き書における職務記述書の作成に関する説明箇所</p>
	<p>日本のサイバーセキュリティ関連の求人票は非常に曖昧に書かれているが、現場が求めている人材を説明するときの物差しになるものが浸透していくことで変わっていくと思う。そのとき、人材像におけるユーザー側とベンダー側の役割の違いを、主な役割が補足に入れるとより理解が進むのではないか。</p>	<p>小規模組織向け手引き書において、基本的な考え方として、委託を踏まえた役割分担を提示。また、今後同様の考え方を踏まえて、大規模組織向け手引き書においても反映予定。</p>	<p>役割の詳細のうち、当該役割を担う人材が所属する組織</p>
	<p>13の分類で最も多いのは「⑧運用管理」と「⑫設計開発」と思う。インフラ系は開発や運用を行う人材の中にセキュリティの専門家がいますが、システム系にはセキュリティの専門家があまりいない。プラス・セキュリティと言ったとき、企業としてシステム開発における業務プロセス企画、アプリ開発やデータベース構築にどのようにフレームワークを適用するか、どのような人材を求めるべきかの視点を入れてほしい。⑧⑫にはサブカテゴリを組み込めると良い。</p>	<p>フレームワーク本体では、汎用的な知識・スキルを役割ごとに整理。そのうえで、各業種業界の組織に特化したスキル・知識の定義については、今後の活用に向けて不断の検討を実施する。</p>	<p>役割の詳細のうち、補足説明</p>
	<p>資料4の21ページのレベルの説明に関して、レベル3の②において、「全て取得している」という表現は厳しい。「おおむね」とか、少々緩い表現が適切ではないか。</p>	<p>御指摘の内容についてフレームワーク本体にて対応済み</p>	<p>レベル定義</p>

手引き書(案)の基本的な考え方についての御意見

項目	御指摘	御指摘を踏まえた対応案	反映箇所(予定)
<p><第2回> 手引き(案) の基本的な考 え方について</p>	<p>企業のサイバーレジリエンスの底上げをするためには、圧倒的に多いユーザー企業のレベルを上げていく必要がある。セキュリティ要件を仕様としてまとめるのはユーザー企業であり、クラウドのセキュリティ機能をどう使うかもユーザーの責任である。そのようなところを大雑把でない形で資料をまとめられるとよい。</p>	<p>ユーザー企業の一例として、小規模組織向け手引き書においてモデルケースを設定し、対応に必要な役割の実施方法を例示 また、クラウドに関しては、運用管理の役割において、必要な知識として追加</p>	<p>大規模組織向け及び小規模組織向け手引き書における役割の説明箇所</p>
	<p>AIが進化する中、5年後ぐらい先にこの手引き書がどのような形で意味を持つのかを考える必要がある。サイバーセキュリティに関するキャリアラダーが見えにくくなっており、若い人たちに対しての一つの指針になるようなものにすべき。</p>	<p>それぞれの役割において、今後のAI活用を見据え、共通的にAI関連で必要な知識・スキルを追加 より高度なAI活用については、AI技術の発展を見ながら、不断の検討を実施する</p>	<p>フレームワーク本体の各役割</p>
	<p>どこまでがフレームワークでどこからが手引き書かは微妙であるが、フレームワークをどう使うかの観点が重要。全てを一気に作れないと思うが、それを順次作っていくというメッセージを出すことが重要である。中小企業向け以外の業種がないので、他業種や大学向け等も順に作るなどもっとバリエーションを増やしてほしい。</p>	<p>手引き書に関して「大規模・小規模事業者」向けだけではなく「教育・個人等」も含めた形で作成する。</p>	<p>各手引き書全体</p>